AB:MWG

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH (1) FACEBOOK USER ID 100002035369849, (2) INSTAGRAM USERNAME "Callme_Tahk" AND (3) INSTAGRAM USERNAME "SW__Gabe," THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK INC.	**TO BE FILED UNDER SEAL** **APPLICATION FOR A SEARCH WARRANT FOR INFORMATION IN POSSESSION OF A PROVIDER (FACEBOOK INC.)** Case No. 19-MJ-1205

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, William J. Schierle, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID and certain Instagram usernames that is stored at premises owned, maintained, controlled or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscribers or customers associated with the user ID and usernames.

2. I am a Detective and Task Force Officer assigned to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") and New York City Police Department ("NYPD") Joint Robbery Task force, and have been since 2015. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been involved in the investigations of numerous cases involving Hobbs Act robberies and related firearms offenses. Through my training, education and experience, I have become familiar with the manner in which evidence of robberies are commonly stored and the manner in which fugitives hide, as well as the uses and capabilities of cellular phones and social media accounts. I have also participated in the execution of search warrants involving evidence of robberies, including searches of electronic devices and social media accounts.

3. I make this affidavit based upon my personal knowledge and my participation in this investigation, including communications with others who have personal knowledge of the events and circumstances described herein; my review of records and reports relating to the investigation; and information gained through my training and experience.

4. The information provided below is for the limited purpose of establishing sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1951 (attempted Hobbs Act robbery) and 924(c) (possessing and discharging a firearm during a crime of violence) (collectively, the "SUBJECT OFFENSES") have been committed by TAHKEM BOYNTON and others.

There is also probable cause to search the information described in Attachment A for evidence of the SUBJECT OFFENSES, as described in Attachment B.

PROBABLE CAUSE

6. On December 23, 2019, at approximately 6:30 p.m., three individuals attempted to rob a convenience store in Staten Island, New York. The attempted robbery was witnessed by the store clerk ("Witness 1") and his two friends, who were in the store with him at the time ("Witness 2" and "Witness 3"). The attempted robbery was also partially captured by video surveillance, which I have reviewed.

7. At the time of the attempted robbery, the three individuals entered the store through the front door. One individual, later identified as TAHKEM BOYNTON, approached Witness 1, brandished a knife and demanded, in sum and substance, "Where's the money? Where's the stash?"

8. A second, unidentified individual ("Co-Conspirator 1") was holding a firearm. A third, unidentified individual wearing a yellow hooded jacket and a hat ("Co-Conspirator 2") was standing near the door and holding the door closed.

9. Below is a still image from video surveillance depicting BOYNTON, Co-Conspirator 1 and Co-Conspirator 2 in the convenience store:

10. Upon entering the convenience store, Co-Conspirator 1 immediately struck Witness 1 above his left eye with the firearm.

11. When Witness 1 refused to give the robbers money or other items, BOYNTON told Co-Conspirator 1 to shoot him. Co-Conspirator 1 then fired four shots in the direction of Witness 1, Witness 2 and Witness 3. None of the shots hit Witness 1 (or anyone else).

12. BOYNTON, Co-Conspirator and Co-Conspirator 2 then left the store without taking money or other items.

13. Law enforcement responded to the scene after receiving a report of shots fired. Law enforcement recovered four nine millimeter shell casings and two fired bullets at the scene.

14. Witness 1, Witness 2 and Witness 3 told law enforcement that they recognized the robber with the knife as an individual who had visited the convenience store frequently.

15. Witness 1 was shown a photo array of six photographs, including a photograph of BOYNTON, and positively identified BOYNTON as the robber who was holding a knife.

16. Witness 2 was shown a photo array of six photographs, including a photograph of BOYNTON, and positively identified BOYNTON as the robber who was holding a knife.

17. Witness 3 was shown a photo array of six photographs, including a photograph of BOYNTON, and positively identified BOYNTON as the robber who was holding a knife.

18. Law enforcement also interviewed an individual ("Individual 1") who lives across the street from the convenience store. BOYNTON lived with Individual 1 at that location for approximately four months until BOYNTON moved out approximately one month ago. Individual 1 was BOYNTON's acquaintance.

19. Individual 1 told law enforcement that if BOYNTON had been with a white male, then the white male must have been someone named "Gabe." Thereafter, law enforcement showed Individual 1 video surveillance of the attempted robbery. Individual 1 recognized Co-Conspirator 2, who is a white male, as "Gabe" by his distinctive yellow jacket, his hat and his manner of walking.

20. Individual 1 used her cellphone to show law enforcement the Instagram home page of Instagram username "SW__Gabe" (the "GABE INSTAGRAM ACCOUNT"). Individual 1 also showed law enforcement a photograph posted by the GABE INSTAGRAM ACCOUNT. The photograph depicts an individual who appears to be the same person as Co-Conspirator 2. Based on Individual 1's statements and my review of the GABE INSTAGRAM ACCOUNT, I believe that the GABE INSTAGRAM ACCOUNT is controlled by Co-Conspirator 2.

21. Individual 1 also used her cellphone to show law enforcement BOYNTON's Instagram account. The Instagram account belonging to BOYNTON has the Instagram username "Callme_Tahk" (the "BOYNTON INSTAGRAM ACCOUNT"). Based on

Individual 1's statements and my review of the BOYNTON INSTAGRAM ACCOUNT, I believe that the BOYNTON INSTAGRAM ACCOUNT is controlled by BOYNTON.

22. Law enforcement has also reviewed a publicly available Facebook page with the username "StayLowKey Tahk" and the unique user ID "100002035369849" (the "BOYNTON FACEBOOK ACCOUNT"). Based upon the username and publicly available photographs posted by the BOYNTON FACEBOOK ACCOUNT, I believe that BOYNTON FACEBOOK ACCOUNT is controlled by BOYNTON.

23. Individual 1 informed law enforcement that BOYNTON communicates with others exclusively via social media platforms, including Facebook and Instagram.

24. Based on my training and experience, I know that individuals who conspire to commit Hobbs Act robberies often communicate both before and after a robbery about the robbery and their whereabouts. In addition, as set forth in more detail below, I know that Facebook and Instagram collect certain location information that would allow law enforcement to determine a user's past locations and patterns of behavior.

25. Accordingly, based on the information set forth in this affidavit, I have probable cause to believe that the information described in Attachment A contains evidence of the SUBJECT OFFENSES, including communications among co-conspirators. I also have probable cause to believe that the information described in Attachment A contains location information that will allow law enforcement to identify common locations and

common patterns of behavior, which will assist law enforcement to identify and locate BOYNTON, Co-Conspirator 1 and Co-Conspirator 2.[1]

TECHNICAL BACKGROUND

26. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos and other information with other Facebook users, and sometimes with the general public.

27. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state and zip code), telephone numbers, screen names, websites and other personal identifiers. Facebook also assigns a user identification number to each account.

28. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with

[1] Through my training and experience, I have become aware of judicial decisions holding that courts may issue search warrants to allow for the collection of evidence that "will aid in the apprehension of a defendant." In re Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013).

individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events and birthdays.

29. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

30. Facebook users can create profiles that include photographs, lists of personal interests and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a

space where the user and his or her "Friends" can post messages, attachments and links that will typically be visible to anyone who can view the user's profile.

31. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

32. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

33. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

34. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as

webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

35. Facebook has a search function that enables its users to search Facebook for keywords, usernames or pages, among other things.

36. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

37. Users may access Facebook on different types of digital devices, such as mobile phones or tablet computers. When a user accesses Facebook on the same digital device using more than one unique user ID, it is possible for Facebook to link all of the accounts associated with those user IDs by "machine cookie ID." In other words, Facebook is able to identify discrete sets of unique accounts that have all accessed Facebook using the same digital device.

38. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender. A poke by one user to another is typically indicative of some sort of social relationship between the two users.

39. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user's access or use of that application may appear on the user's profile page. Based on my training and experience, suspects sometimes use Facebook apps, which sometimes themselves have internal messaging capability, to communicate with other individuals.

40. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles and other items; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

41. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

42. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments

associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

43. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events

relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

44. Instagram is a free-access social networking website that can be accessed at http://www.instagram.com. Instagram allows its users to establish accounts. Instagram was developed and operated by a company of the same name, and was acquired by Facebook. Users can also log into Instagram using an existing Facebook account. Users can then use their accounts to share photographs with other Instagram users, and sometimes with the general public. Users can also attach captions (brief textual descriptions) of photographs that are shared along with the photographs.

45. Instagram asks users to provide basic contact and personal identifying information to Instagram, either during the registration process or thereafter. This information may include the user's full name, gender, contact email addresses, Instagram password, telephone numbers, a personal biography, websites, an account photograph, and other personal identifiers.

46. Instagram users can choose to "follow" other Instagram users. In most cases, any photographs posted by an Instagram user are instantly visible to all of their "followers."

Followers can also comment on other users' photographs, and "like" other users' photographs. This "like" feature allows users to give positive feedback on particular photographs. Instagram users also have the ability to "tag" (i.e., label) other Instagram users in a photograph or video.

47. Instagram users can choose to make their profiles "private," in which case they must approve other users' requests to "follow" them. If a user's profile is not "private," any other user may follow them – and see their posted photographs – without their knowledge or approval.

48. Photographs on Instagram may contain "metadata," which is technical data embedded into the photographs themselves by users before uploading them to Instagram. Users may choose to attach additional Metadata to photographs after they have been uploaded to Instagram. Metadata can include, but is not limited to, the time at which a photograph was taken, the device that was used to take the photograph, and the latitude and longitude at which the photograph was taken.

49. Instagram also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Instagram, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views an Instagram profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

50. Instagram also retains logs of the device identifiers or any mobile device that a user uses to connect to Instagram. These identifiers uniquely identify each mobile device. These logs may contain information about the actions taken by the user ID or device

identifier on Instagram, including information about the type of action, the date and time of the action, and the user ID and device identifier associated with the action. For example, if a user views an Instagram profile, that user's device identifier log would reflect the fact that the user viewed the profile, and would show when and from what device identifier the user did so.

51. Social networking providers like Instagram typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Instagram users may communicate directly with Instagram about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Instagram typically retain records about such communications, including records of contracts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communication.

52. For the reasons set forth herein, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook and Instagram, such as account access information, transaction information and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

53. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other

information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

54. Based on the forgoing, I request that the Court issue the proposed search warrant.

55. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

57. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal

these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

WILLIAM J. SCHIERLE
Detective/Task Force Officer
NYPD/ATF Joint Robbery Task Force

Subscribed and sworn to before me on December 30, 2019

HONORABLE STEVEN L. TISCIONE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook account associated with (1) Facebook user ID 100002035369849, (2) Instagram username "Callme_Tahk" and (3) Instagram username "SW__Gabe," that is stored at premises owned, maintained, controlled or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. For the avoidance of doubt, the property to be searched includes information associated with any and all accounts linked by machine cookie ID to (1) Facebook user ID 100002035369849, (2) Instagram username "Callme_Tahk" and (3) Instagram username "SW__Gabe."

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID and username listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook or Instagram activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook or Instagram applications;

(e) All communications or other messages sent or received by the user of the account using the Instagram Direct feature or any other feature that allows the user to send and receive private messages;

(f) All other records of communications and messages made by, received by or associated with the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook or Instagram posts and all non-Facebook webpages and content that the user has "liked";

(j) All past and present lists of friends or followers created by the account;

(k) All records of searches performed by the account;

(l) The types of service used by the user;

(m) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(n) All privacy settings and other account settings, including privacy settings for individual posts and activities, and all records showing which users have been blocked by the account; and

(o) All records pertaining to communications between Facebook or Instagram and any person regarding the user or the user's account, including contacts with support services and records of actions taken;

(p) All records of Instagram accounts used to log into the users' Instagram accounts, including the Instagram identification numbers of those accounts and any other related Instagram information associated with the users' Instagram accounts.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1951 (attempted Hobbs Act robbery) and 924(c) (possessing and discharging a firearm during a crime of violence) (collectively, the "SUBJECT OFFENSES") involving TAHKEM BOYNTON, Co-Conspirator 1 and Co-Conspirator 2 from since December 1, 2019 to the present, including, for each user ID and username identified in Attachment A, information pertaining to the following matters:

(a) Comments, communications, photographs and images concerning the SUBJECT OFFENSES;

(b) Associations and communications with and between TAHKEM BOYNTON, Co-Conspirator 1, Co-Conspirator 2, and any other individuals involved in the attempted robbery described in the affidavit;

(c) Evidence indicating the past locations of TAHKEM BOYNTON, Co-Conspirator 1, Co-Conspirator 2, and any other individuals involved in the attempted robbery described in the affidavit;

(d) Evidence indicating how and when each account identified in Attachment A was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the SUBJECT OFFENSES under investigation and to the account owner;

(e) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and

(f) The identity of the person(s) who created or used the user ID or username, including records that help reveal the whereabouts of such person(s).